

Alerta de seguridad informática	8FFR20-00213-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2020
Última revisión	11 de Febrero de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado la activación de cuatro portales fraudulentos asociados a una IP que suplanta el sitio web oficial del **Banco Scotiabank**, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URLs

scotia[.]chile[.]com[.]cl01[.]online
 scotia[.]chile[.]com[.]cl01[.]online/portalesempresas/
 scotia[.]chile[.]com[.]cl01[.]online/login/personas/
 scotia[.]chile[.]com[.]cl01[.]online/movil/

Domain cl01.online																	
cl01 / online / Subdomains																	
record type	TTL	value															
A	7207	165.22.216.114															
NS	172800	ns1.dnsowl.com	Zones on DNS server 185.34.216.159, 198.251.84.16, 104.207.141.138														
NS	172800	ns2.dnsowl.com	Zones on DNS server 64.32.22.100, 168.235.75.52, 45.32.237.128														
NS	172800	ns3.dnsowl.com	Zones on DNS server 45.63.106.63, 45.63.5.234, 209.141.39.150														
SOA	172800	<table border="1"> <tr><td>Mname</td><td>ns1.dnsowl.com</td></tr> <tr><td>Rname</td><td>hostmaster.dnsowl.com</td></tr> <tr><td>Serial number</td><td>1581344216</td></tr> <tr><td>Refresh</td><td>7200</td></tr> <tr><td>Retry</td><td>1800</td></tr> <tr><td>Expire</td><td>1209600</td></tr> <tr><td>Minimum TTL</td><td>600</td></tr> </table>		Mname	ns1.dnsowl.com	Rname	hostmaster.dnsowl.com	Serial number	1581344216	Refresh	7200	Retry	1800	Expire	1209600	Minimum TTL	600
Mname	ns1.dnsowl.com																
Rname	hostmaster.dnsowl.com																
Serial number	1581344216																
Refresh	7200																
Retry	1800																
Expire	1209600																
Minimum TTL	600																

Ilustración 1 Dominio donde se Aloja Url del Banco Scotiabank, Falso y DNS que utiliza

Certificados

Subject DN	CN=www1.scotia.chile.com.cl01.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	285935458906880461733965190302654597704339
Validity	2020-02-08 19:00:16 to 2020-05-08 19:00:16 (90 days, 0:00:00)
Names	www1.scotia.chile.com.cl01.online

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank

IP
165[.]22[.]216[.]114

Domain <u>scotia.chile.com.cl01.online</u> is located on IP address << 165.22.216.114 >>	
Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices
City	Seattle
Region/State	Washington
Country	 US , United States
Reg. date	1993-03-31
Host name	no record in reverse zone
Domains	1 scotia.chile.com.cl01.online

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Scotiabank

Localización
India Bangalore, Karnataka

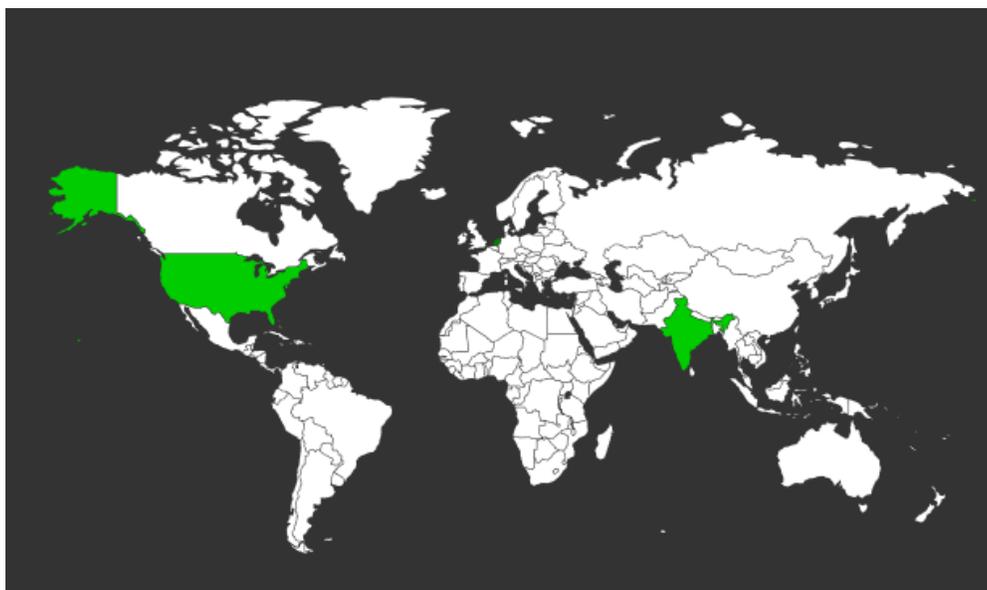
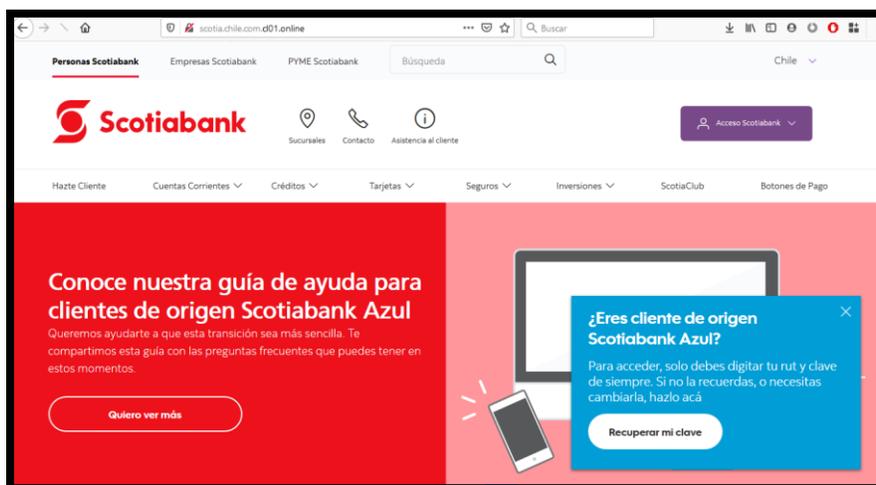


Imagen del sitio



Whois

```

Domain Name: CL01.ONLINE
Registry Domain ID: D170067396-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-02-08T18:31:12.0Z
Creation Date: 2020-02-08T18:29:14.0Z
Registry Expiry Date: 2021-02-08T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
  
```

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido hacia la URL maliciosa.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.